Sandia National Laboratories
Safeguards & Security Awareness
Annual Security Refresher Briefing

ANNUAL SECURITY REFRESHER BRIEFING

SEC100:
Annual Security Refresher Briefing

Interactive version on the SON available at
https://prod-ng.sandia.gov/wbt/SEC100/intro.html

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2023-03263 O v3.0 7.24.2023

ADDITIONAL RESOURCES

- Getting Started with Classified
- Understanding Classification
- Non-DC Responsibilities
- How to Read a Classification Guide
- Security Message: Export Control
- Security Message: Microsoft Teams
- Who and What Can Go Where?
- Mobile Devices and Secure Space
- Critical Information Lists (CILs)
- DOE & Sandia Reporting Requirements FAQs
- Controlled Articles at Sandia

INTRODUCTION

Hello everyone,

I'm David Gibson, your Deputy Labs Director and Chief Operating Officer and I'm here to talk about Safeguards & Security. My Sandia career has spanned 22 years in New Mexico, Washington DC, and California in fields as diverse as nuclear weapons, infrastructure operations, and quality programs. I started as a student intern and have worked as a staff member, team lead, manager, senior manager, director and now Deputy Labs Director and Chief Operating Officer.

We are recognized all over the world as a premiere national security laboratory. We are all privileged to be a part of Sandia's national security legacy and with that privilege our responsibility to protect our Nation's most sensitive information must be everyone's priority.

Sandia's mission is critical as the world enters a new nuclear weapons era. Other countries are actively building their nuclear arsenal and posing a serious and dangerous threat to U.S. National security.

Physical, technical, personnel, and information security continue to be top priority at for Sandia. The country needs us to remain diligent in our focus on security protocols. A hybrid work environment makes information security a challenge in the year ahead. The adversaries are standing by waiting to exploit any and every opening to understand, influence, and undermine what we do here.

This year's Annual Security Refresher Briefing will focus on information protection. We continue to experience Unauthorized Network-based Transmissions, our most concerning type of security incident. DOE and Sandia's leadership are working to reduce those incidents but we need your help. We continue to see reports of mobile devices being taking into Secure Spaces. Again, we need your help to curtail these security breaches.

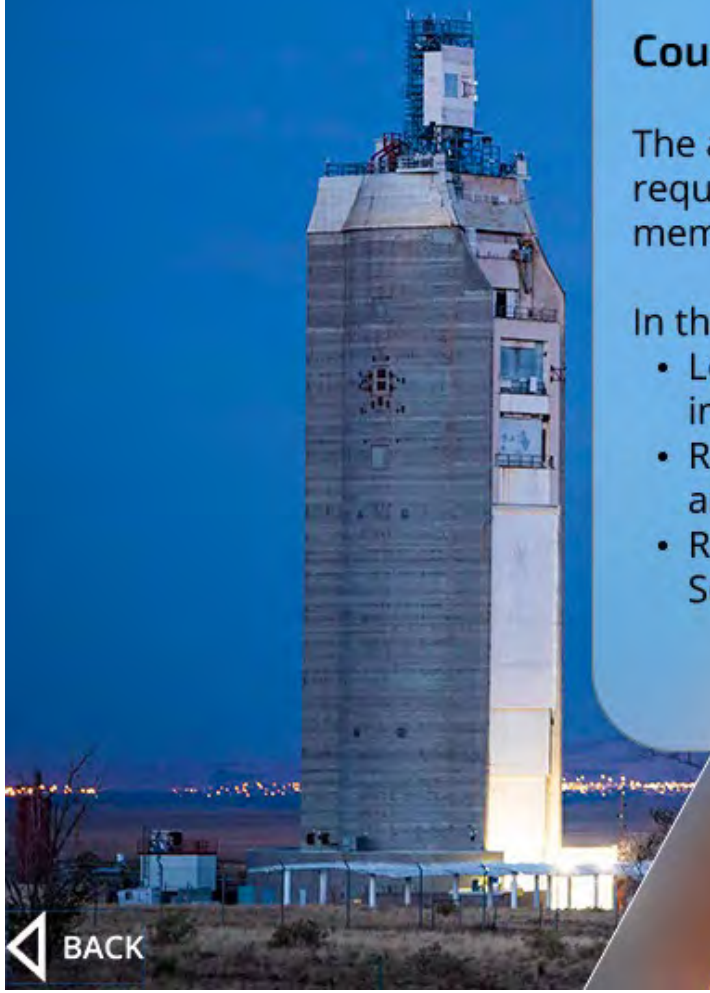
Sandia's security culture is unparalleled, and we have teams of security professionals ready to help. Please pay close attention to the scenarios in this year's refresher and think about areas where you might be vulnerable, then work with your security partners to close the loopholes.

Security begins and ends with you and me. We must pay attention to security every day, in every email, every conversation, and every document.

I challenge you to focus on your security responsibilities in the upcoming year knowing that the nation and the world are watching and depending on us to provide exceptional service in the national interest.

Thank you.

--David Gibson



Course Objective:

The annual security refresher briefing is required by DOE O 470.4B for all cleared members of the workforce (MOWs).

In this briefing, you will:

- Learn about Sandia-specific security incidents and how to prevent recurrence.
- Review your security responsibilities and best practices.
- Receive Counterintelligence and Security updates.

COURSE MODULES

CC

Sandia sends approximately 8000 computing systems to Reapplication per year.

Ally Gater's team has been relocated to a Vault-Type Room (VTR). At her new desk, Ally found an old classified computer with the classified markings removed and a sticky note that read 'Hard drive removed'. Her manager told her to get rid of it.

What should Ally do? Choose an answer below.

Ally should submit a ticket to Reapplication so that the computer can be reused.

Ally should contact the Corporate Computing Help Desk (CCHD) for identifying the appropriate point-of-contact for determining if the computer is cleared of classified.

BACK

Ally Gater's team has been relocated to a Vault-Type Room (VTR). At her new desk, Ally found an old classified computer with the classified markings removed and a sticky note that read 'Hard drive removed'. Her manager told her to get rid of it.

What should Ally do? Choose an answer below.

Congratulations, you chose correctly. Ally should contact CCHD!

INCIDENTS OF SECURITY CONCERN (IOSC) AT SANDIA

Category A: may involve the loss, theft, suspected compromise, or compromise of departmental assets.

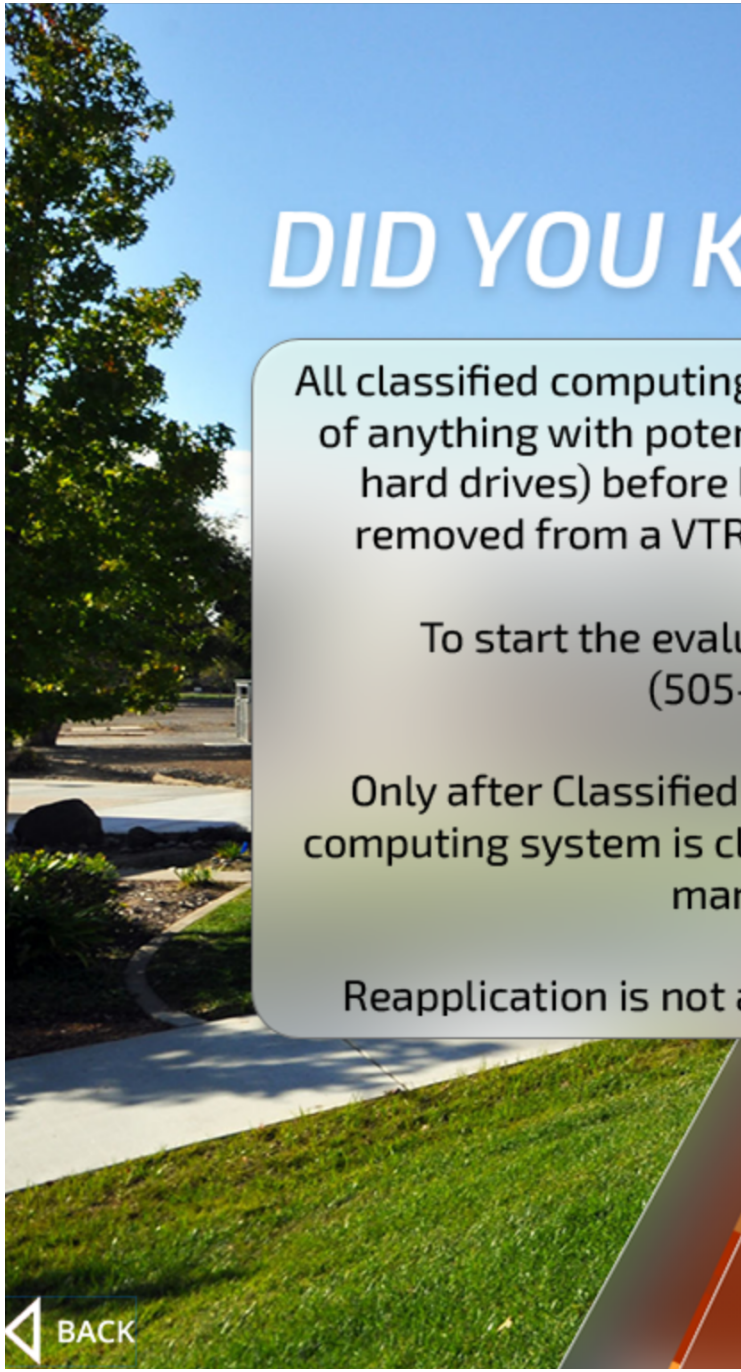
Category B: may involve failure to adhere to security procedures where the likelihood of compromise is ***remote*** or ***not suspected***.

DID YOU KNOW?

Discussing the details of a classified security incident outside of a limited area, or via unsecured means, could result in ***a subsequent security incident.***

Ally sent the computer to Reapplication – after all, if her team didn't need it, surely someone else would. She was later contacted by an Inquiry Official from the Security Incident Management Program (SIMP), who had begun a SIMP Inquiry. The inquiry found that the computer she sent to Reapplication contained a second, small solid state hard drive. This classified drive had been removed from the VTR and transported to Reapplication, where it was improperly stored unattended in a Property Protection Area (PPA) for several days.

This incident was categorized as a Category A Incident of Security Concern (IoSC).



DID YOU KNOW?

All classified computing systems must be evaluated and cleared of anything with potential to store classified information (e.g., hard drives) before being destroyed, reused, permanently removed from a VTR or safe, and/or sent to Reapplication.

To start the evaluation process, you must call CCHD (505-845-2243, option 1+1).

Only after Classified CCHD personnel have verified that the computing system is cleared of classified can the equipment be managed as unclassified.

Reapplication is not authorized to receive classified matter.

Think:

Do I need to ***permanently*** remove computing equipment from a Vault-Type Room (VTR) and/or a GSA security container (safe)?

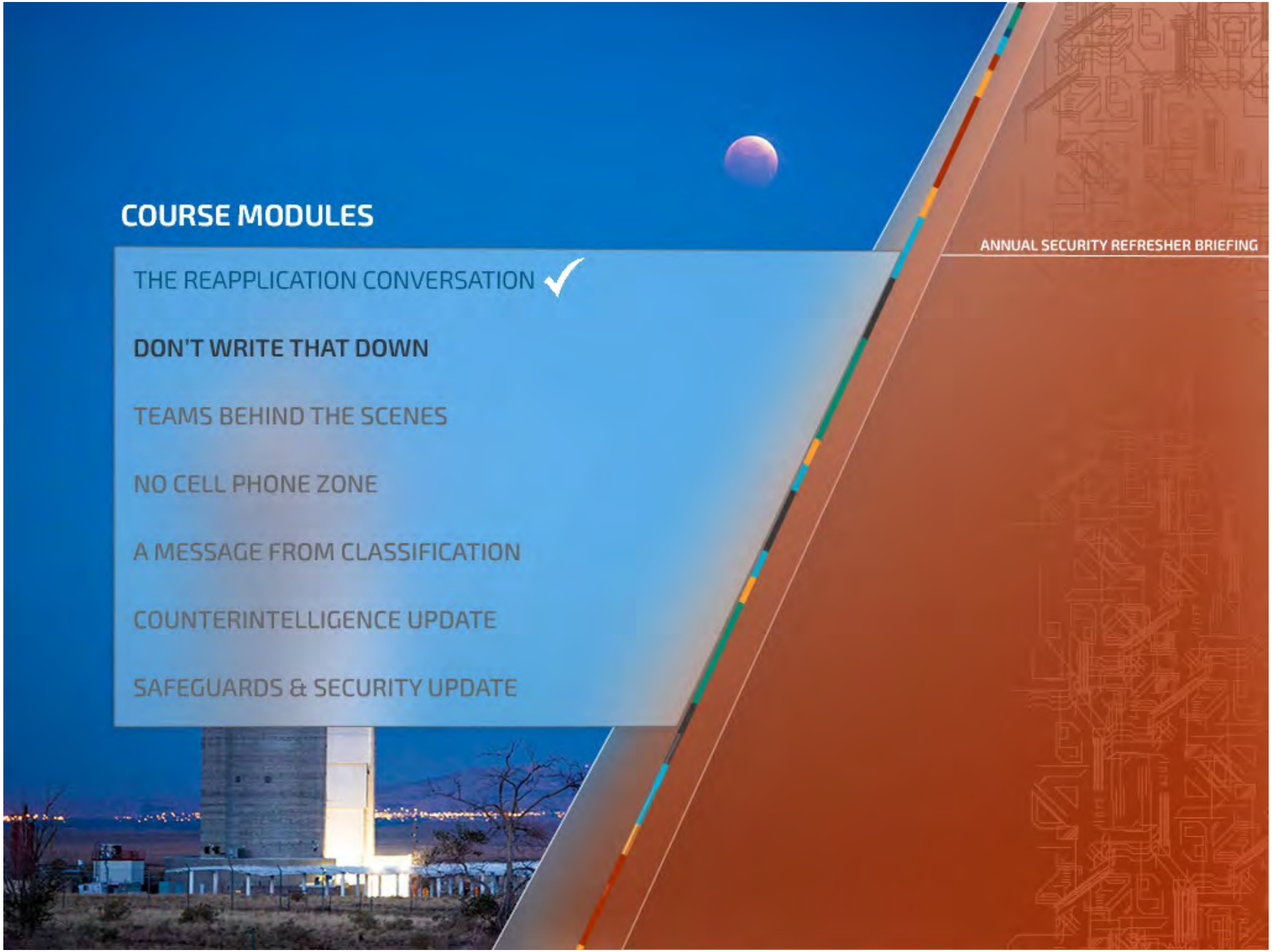
Assess:

Computing equipment that is in a safe or VTR may be classified matter because it may have processed classified information and/or been connected to a classified system or network.

Am I sure I can remove it from the safe or VTR?

Protect:

Treat any and all classified processing equipment as classified matter. Do not remove this equipment from a VTR or safe without contacting CCHD for assistance.


COURSE MODULES
THE REAPPLICATION CONVERSATION
DON'T WRITE THAT DOWN
TEAMS BEHIND THE SCENES
NO CELL PHONE ZONE
A MESSAGE FROM CLASSIFICATION
COUNTERINTELLIGENCE UPDATE
SAFEGUARDS & SECURITY UPDATE
ANNUAL SECURITY REFRESHER BRIEFING

Sandia's Security Incident Management Program (SIMP) includes 7 Inquiry Officials in New Mexico and 2 in California

Allen Faybet is a Q-cleared electrical engineer and subject matter expert (SME) who had recently returned home to California from a trip to New Mexico, where he was consulting on a new classified application of a device developed by Al's team. A few weeks later, Al was using the notes he captured in his notebook to brief his team about what he learned on his trip. After the meeting, his Derivative Classifier (DC) stopped him in the hall to review his notebook, and advised him that some of his notes contained classified information and that he needed to report to SIMP.

What went wrong for Al Faybet?

Al did not have a need-to-know for the classified information from his trip.

Al's notebook contained classified information and should have been protected as classified.

Allen Faybet is a Q-cleared electrical engineer and subject matter expert (SME) who had recently returned home to California from a trip to New Mexico, where he was consulting on a new classified application of a device developed by Al's team. A few weeks later, Al was using the notes he captured in his notebook to brief his team about what he learned on his trip. After the meeting, his Derivative Classifier (DC) stopped him in the hall to review his notebook, and advised him that some of his notes contained classified information and that he needed to report to SIMP.

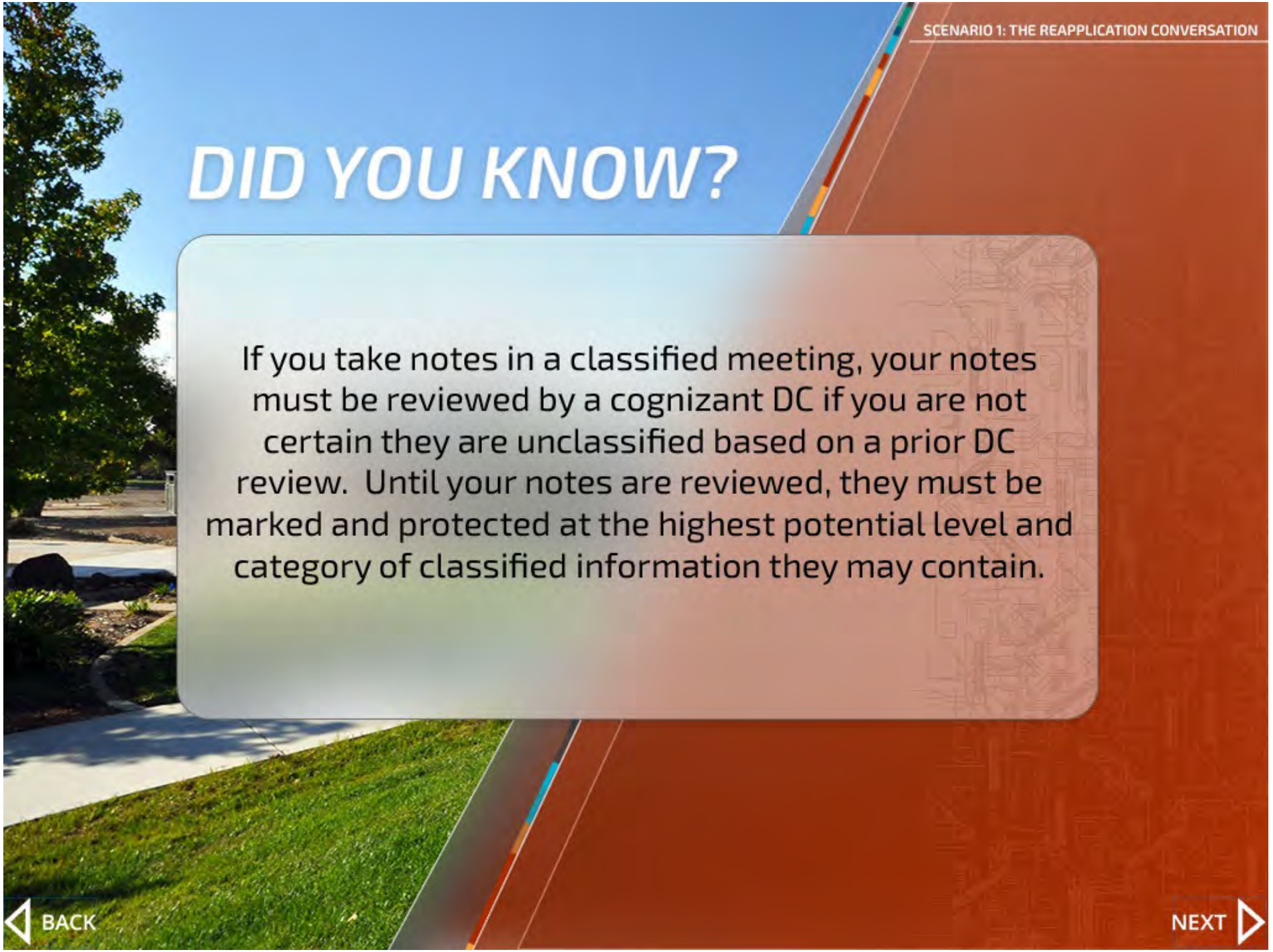
What went wrong for Al Faybet?

Congratulations, you chose correctly. Al's notebook contained classified that needed to be protected.

While attending a classified meeting in New Mexico, Al had captured a few notes in his notebook. This was the same notebook he used at home to meet with his team. Although he isn't a DC, Al didn't think he captured classified information.

A SIMP Inquiry was conducted. A review of Al's notebook determined that it contained Secret Restricted Data (SRD). Although Al was appropriately authorized for the information, the notebook was left unattended and unsecured in his hotel room, home, and his Limited Area office.

The event was categorized as a Category A IoSC.



DID YOU KNOW?

If you take notes in a classified meeting, your notes must be reviewed by a cognizant DC if you are not certain they are unclassified based on a prior DC review. Until your notes are reviewed, they must be marked and protected at the highest potential level and category of classified information they may contain.

Think:

Do I work in a potentially classified subject area or engage in classified meetings or discussions?

Assess:

If I take notes in a classified setting, they must be treated as classified until reviewed by a DC. Who is the DC for this information? Where will it be stored or destroyed?

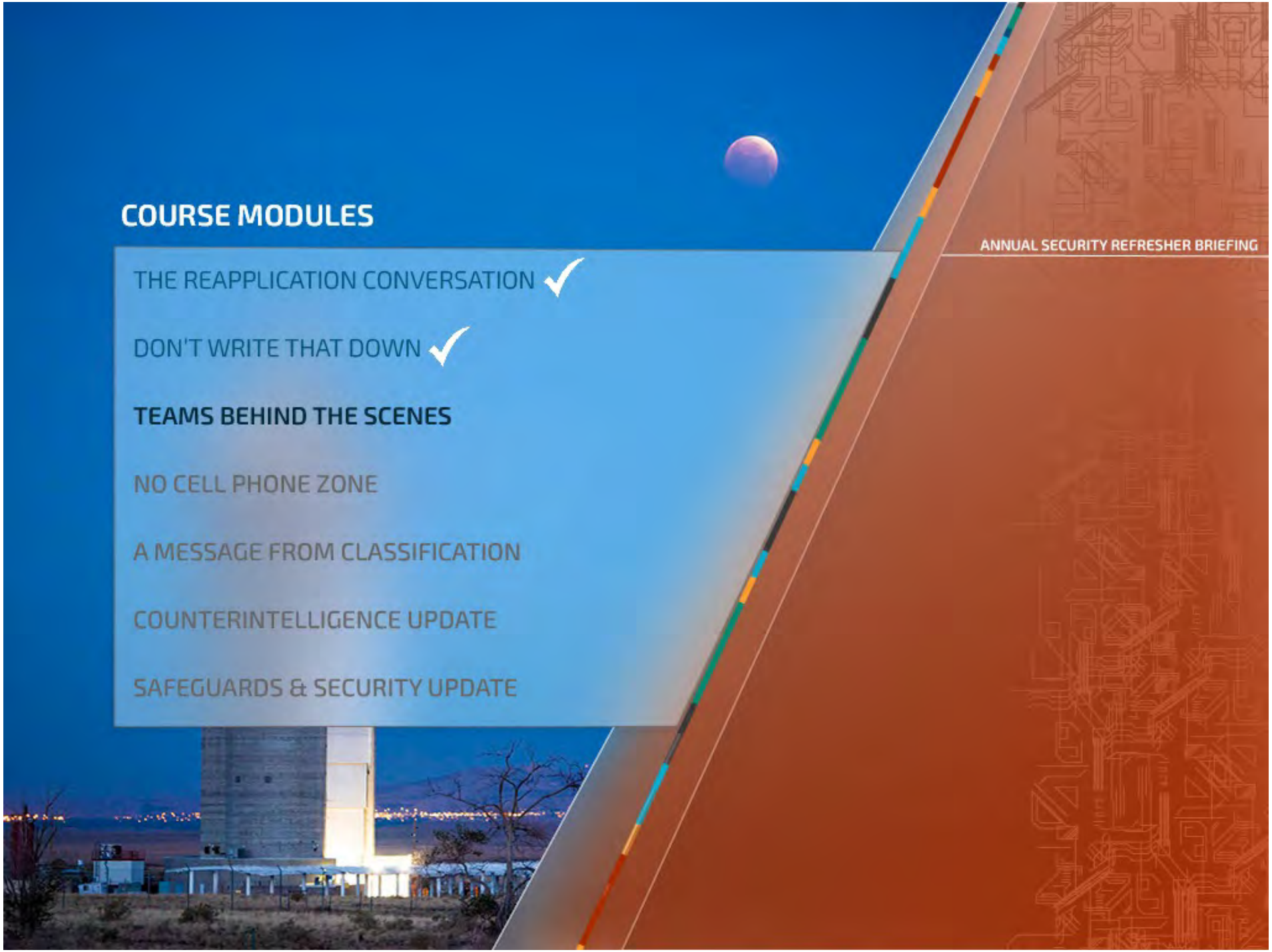
Protect:

Ask before you ***act!***

Ensure you know your DC, clearly mark your notebook, and store your notes in an approved safe or VTR.

BACK

NEXT


COURSE MODULES
THE REAPPLICATION CONVERSATION
DON'T WRITE THAT DOWN
TEAMS BEHIND THE SCENES
NO CELL PHONE ZONE
A MESSAGE FROM CLASSIFICATION
COUNTERINTELLIGENCE UPDATE
SAFEGUARDS & SECURITY UPDATE
ANNUAL SECURITY REFRESHER BRIEFING

On average, Sandians participate in over 5900 Microsoft Teams meetings every day.

Rhea Lize works from home as a Q-cleared financial analyst and is supporting a large project including both classified and unclassified work. After a major deliverable, Rhea was one of many who used Teams to call into a project update meeting held onsite in a large conference room. After the call, Rhea realized that one of the attendees was a foreign national postdoc, and that the presentation included drawings marked as export controlled information (ECI).

What should Rhea do?

Don't worry about it. The scientist is part of the project after all.

Immediately contact SIMP to report a potential incident.

Rhea Lize works from home as a Q-cleared financial analyst and is supporting a large project including both classified and unclassified work. After a major deliverable, Rhea was one of many who used Teams to call into a project update meeting held onsite in a large conference room. After the call, Rhea realized that one of the attendees was a foreign national postdoc, and that the presentation included drawings marked as export controlled information (ECI).

What should Rhea do?

Congratulations, you chose correctly.
Rhea should contact SIMP immediately.

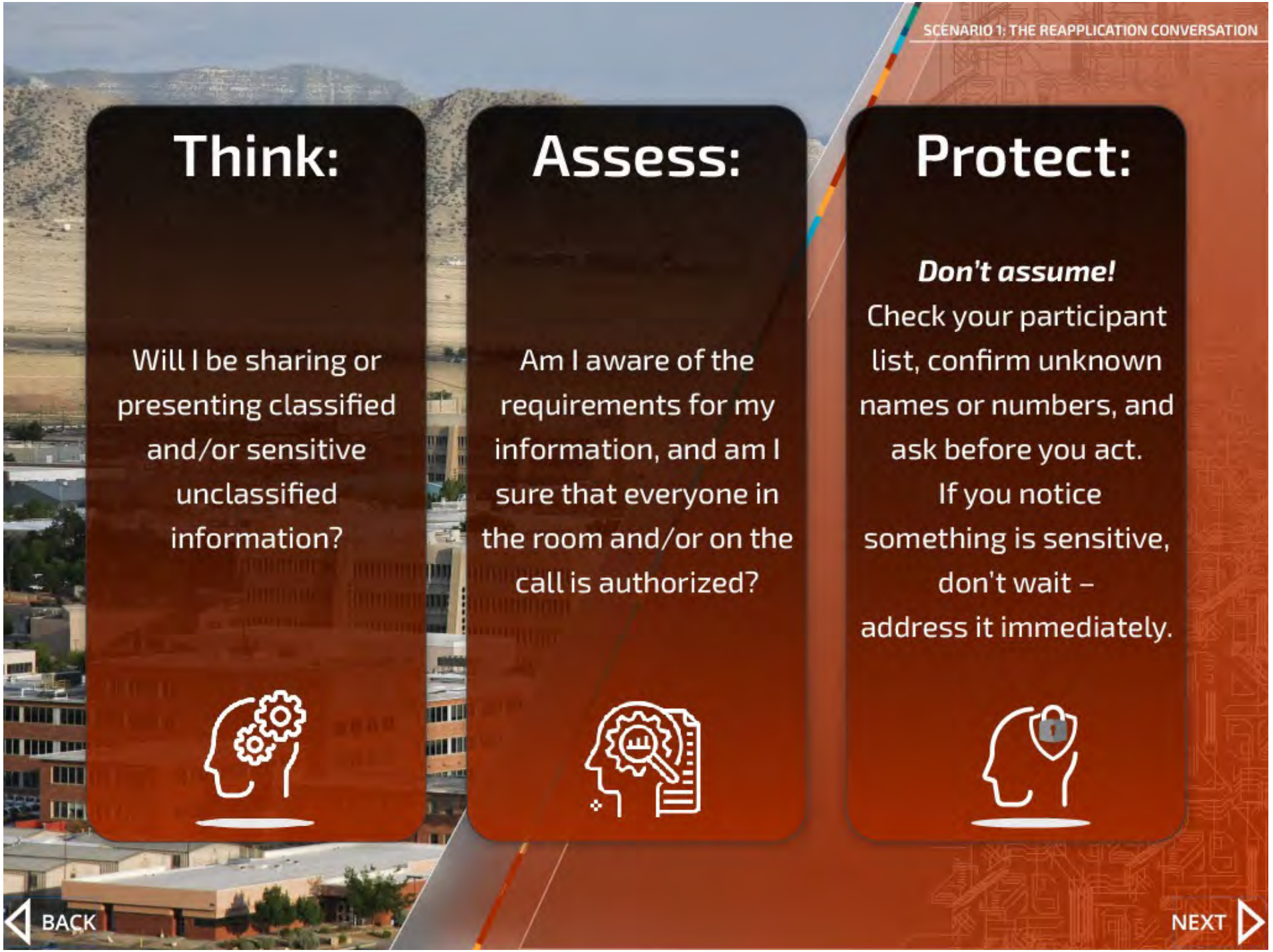
Rhea called SIMP to report her concerns and a SIMP inquiry was conducted. The inquiry found that the meeting included on-site and virtual attendees. The presenter was certain that all persons in the conference room were authorized for the information. However, they were not familiar with most of the people calling in, but had assumed that anyone invited was also authorized. The SIMP inquiry determined that the presentation contained export controlled information and that the scientist attending virtually was not authorized for the information.

This event was categorized as a Category B IoSC.

DID YOU KNOW?

While it is important to team with others for great results, you must ensure that everyone on the call and/or in the room is authorized for the information you are sharing.

If you don't know, ask!



Think:

Will I be sharing or presenting classified and/or sensitive unclassified information?

Assess:

Am I aware of the requirements for my information, and am I sure that everyone in the room and/or on the call is authorized?

Protect:

Don't assume!

Check your participant list, confirm unknown names or numbers, and ask before you act.

If you notice something is sensitive, don't wait – address it immediately.

BACK

NEXT

COURSE MODULES

ANNUAL SECURITY REFRESHER BRIEFING

- THE REAPPLICATION CONVERSATION ✓
- DON'T WRITE THAT DOWN ✓
- TEAMS BEHIND THE SCENES ✓
- **NO CELL PHONE ZONE**
- A MESSAGE FROM CLASSIFICATION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE

There are over 17,000 clearance holders at Sandia that include more than 2,500 contractors.

Software engineer Samuel Sung works for a large defense contractor that has partnered with Sandia for many years. Recently, he was required to come on site to assist in some classified work. Sam hadn't been on site for a few years, but he knew that the rules were changed for mobile devices since he was last here, and knew that they had to be stored while in the Limited Area and before discussing classified information. After a classified meeting, Sam was told he should report to SIMP that he had his personally-owned phone – even though he had been sure to place it in the storage box he found on the wall outside the conference room.

What do you think Sam Sung did wrong?

Only mobile devices owned by Sandia are allowed to be stored inside a Limited Area building.

The box Sam used was not an approved storage location.

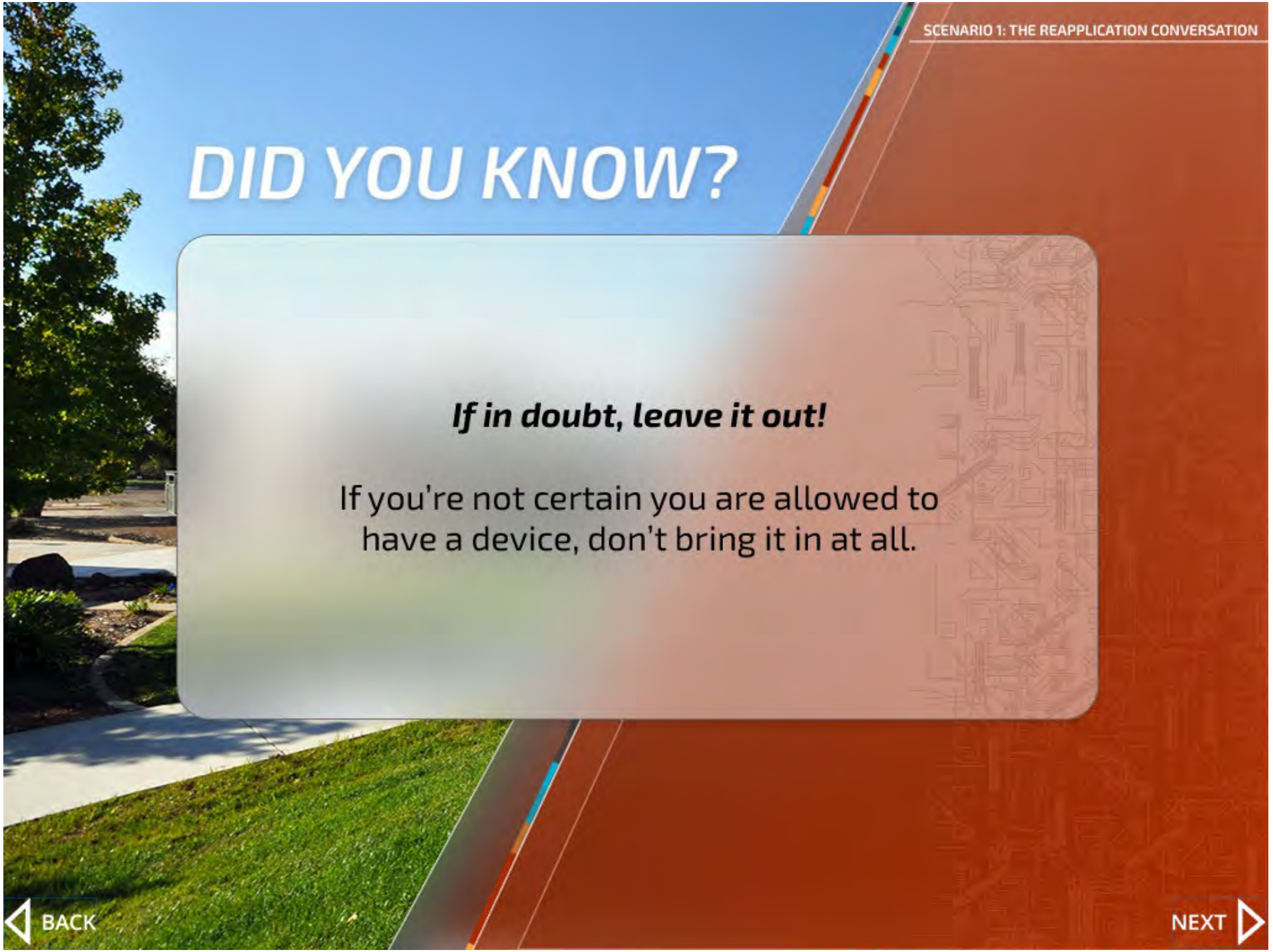
Software engineer Samuel Sung works for a large defense contractor that has partnered with Sandia for many years. Recently, he was required to come on site to assist in some classified work. Sam hadn't been on site for a few years, but he knew that the rules were changed for mobile devices since he was last here, and knew that they had to be stored while in the Limited Area and before discussing classified information. After a classified meeting, Sam was told he should report to SIMP that he had his personally-owned phone – even though he had been sure to place it in the storage box he found on the wall outside the conference room.

What do you think Sam Sung did wrong?

Congratulations, you chose correctly.
Sam did not store his device in an approved storage location.

Sam called SIMP to report, and a SIMP inquiry was conducted. The inquiry determined that Sam brought his phone into Secure Space, and placed it in a legacy, unapproved storage box directly outside the conference room. This box was not a designated, approved storage location for mobile devices and was inside Secure Space. The inquiry found Sam's mobile device was in aural proximity to a classified discussion while in this meeting. Everyone in the meeting was appropriately cleared and the inquiry found that there was no active call or recording.

The event was categorized as a Category B IoSC.



DID YOU KNOW?

If in doubt, leave it out!

If you're not certain you are allowed to have a device, don't bring it in at all.

Think:

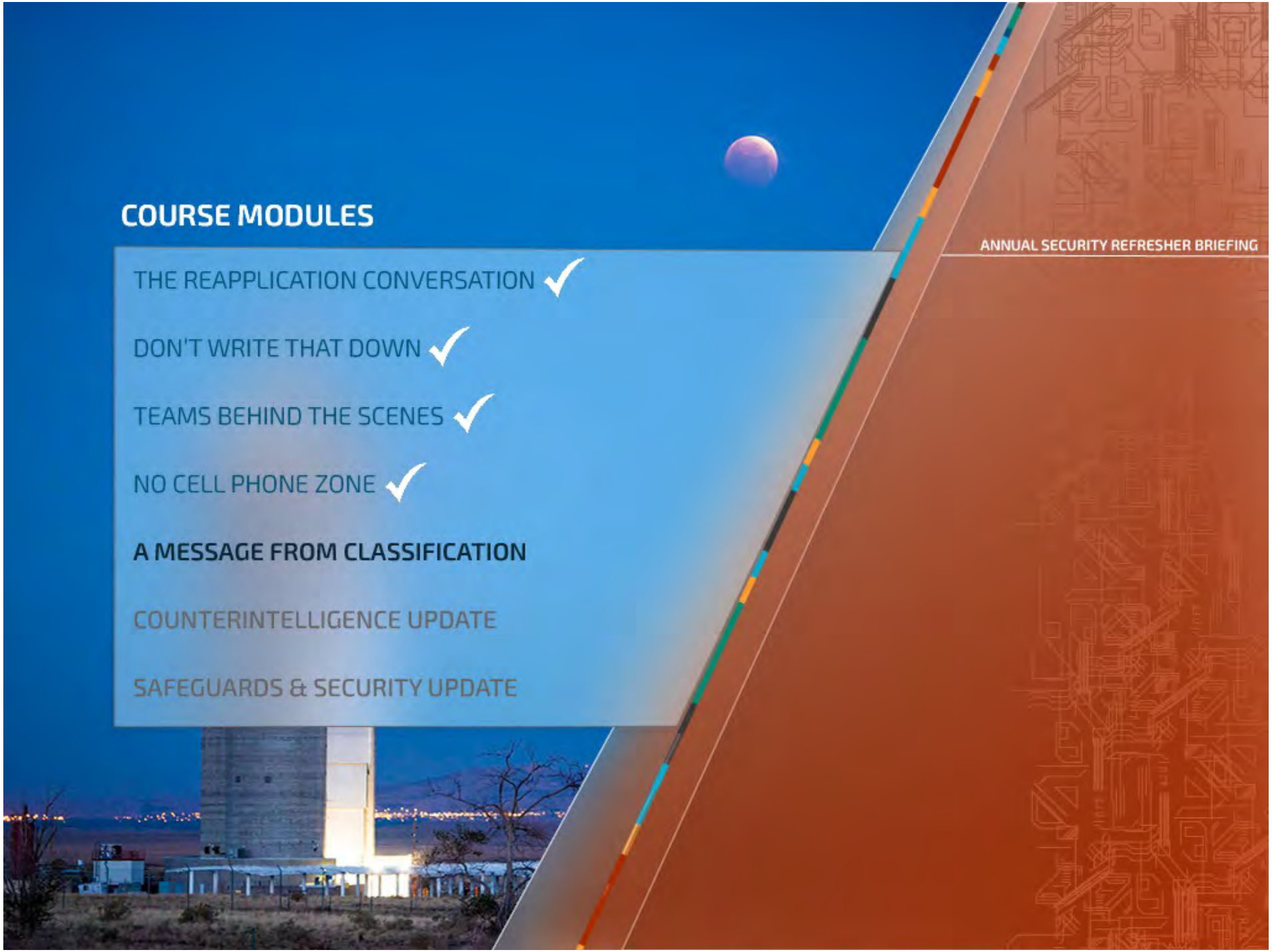
Do I know what the current rules are for mobile devices while on Sandia-controlled premises?

Assess:

Where are you going?
What are your devices?
What capabilities do they have?
Who owns them?

Protect:

Ensure that you understand mobile device policies. Contact Security Connection for assistance and ask your manager, colleagues or Sandia partner for guidance – especially if you haven't been on-site in awhile.


COURSE MODULES
THE REAPPLICATION CONVERSATION
DON'T WRITE THAT DOWN
TEAMS BEHIND THE SCENES
NO CELL PHONE ZONE
A MESSAGE FROM CLASSIFICATION
COUNTERINTELLIGENCE UPDATE
SAFEGUARDS & SECURITY UPDATE
ANNUAL SECURITY REFRESHER BRIEFING

A MESSAGE FROM THE CLASSIFICATION OFFICE

A Derivative Classifier (DC) is an individual authorized to confirm that an unmarked document or material is unclassified, or determine that it is classified as allowed by his or her letter of authority. A DC can also determine that a previously marked document needs to be classified at a higher level and/or category.

A Derivative Declassifier (DD) is an individual authorized to declassify or downgrade Sandia-originated documents, equipment or material as allowed by his or her letter of authority. DDs are located in the Classification Office.

You can locate a DC or DD through Jupiter application (jupiter.sandia.gov).

For Questions:
NM: classificationdept@sandia.gov
CA: CAClassDept@sandia.gov

When requesting a DC review, do not transmit on an unclassified network. Start on the Sandia Classified Network (SCN). If a DC determines your material to be unclassified, use the Downshift utility to move it to the Sandia Restricted Network (SRN).

A MESSAGE FROM THE CLASSIFICATION OFFICE

You must request a DC review for:

- A newly generated document or material in a potentially classified subject area.
- An existing, unmarked document or material you believe may contain classified information.
- An existing, marked document or material you believe may contain information classified at a higher level or more restrictive category.
- A newly generated document that consists of a complete section (e.g., chapter, attachment, appendix) taken from another classified document.
- Upgrading the classification level and/or category of information, documents, or material based on proper guidance.

A MESSAGE FROM THE CLASSIFICATION OFFICE

Declassification review by a DD must occur when the document or material is:

- Prepared for declassification in full.
- Prepared as redacted versions.
- Requested under statute or Executive Order (i.e., declassification for public release).
- Referred to DOE by other government agencies that are or identified as potentially containing RD/FRD/TFNI.
- Marked for declassification prior to actual declassification to ensure that National Security Information (NSI) document or material does not contain classified information.
- An NSI document or material that is a permanent historical record that is 25 years old or older.

You can locate a DD or a DC via Jupiter on the Sandia Restricted Network (SRN) at jupiter.sandia.gov.

A MESSAGE FROM THE CLASSIFICATION OFFICE

If you believe a DC determination is incorrect, you have the responsibility to challenge the determination.

For assistance with challenges, contact the classification office:

In New Mexico: (505) 844-5574 / classificationdept@sandia.gov
In California: CAClassDept@sandia.gov

You are encouraged to resolve challenges locally in discussions with your DC and the Classification Officer. If it cannot be resolved you have the right, at any time, to submit a formal written challenge to the DOE Office of Classification Director. Request additional information from outreach@hq.doe.gov. Under no circumstances will you be subject to retribution for making such a challenge. See Laboratory Policy SS002, Identifying Classified Information, Section 4 for Challenge procedures.

You can locate a DD or a DC via Jupiter on the Sandia Restricted Network (SRN) at jupiter.sandia.gov.

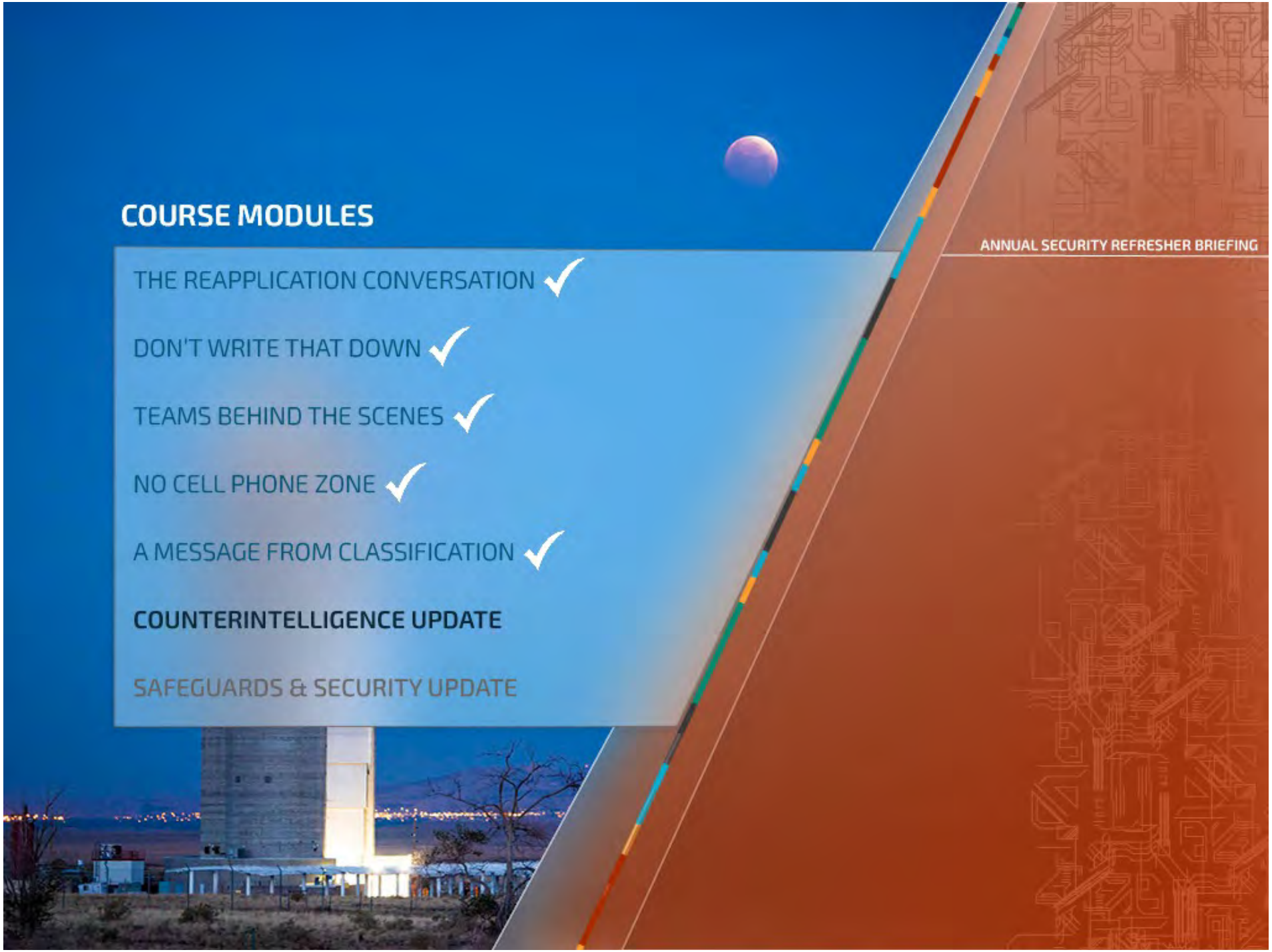
A MESSAGE FROM THE CLASSIFICATION OFFICE

The GEN-16 REVISION 2: "NO COMMENT" POLICY

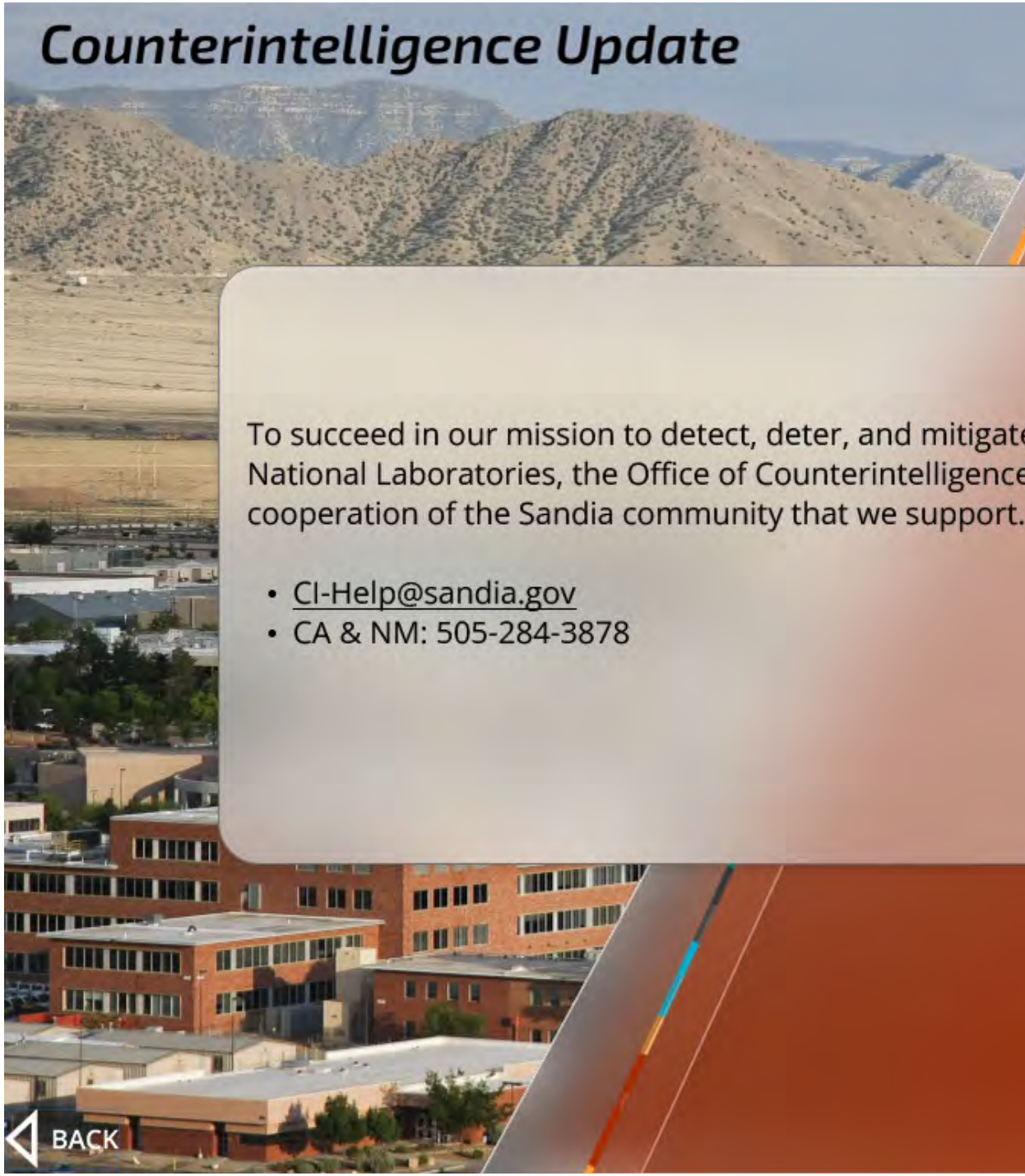
The GEN-16 policy applies to classified information in the open literature. You can't prevent classified information that is outside of your control from appearing in the public but cleared individuals must not comment on it.

A comment is any activity (not just verbal) that would allow a person who is not authorized access to classified information to locate the information or confirm the classified nature or technical accuracy of the information.

Even if you didn't know the information is classified, you are responsible for not drawing attention to it. Never assume that information in classified subject areas found in public venues is unclassified.


COURSE MODULES
THE REAPPLICATION CONVERSATION
DON'T WRITE THAT DOWN
TEAMS BEHIND THE SCENES
NO CELL PHONE ZONE
A MESSAGE FROM CLASSIFICATION
COUNTERINTELLIGENCE UPDATE
SAFEGUARDS & SECURITY UPDATE
ANNUAL SECURITY REFRESHER BRIEFING

Counterintelligence Update



To succeed in our mission to detect, deter, and mitigate threats to Sandia National Laboratories, the Office of Counterintelligence (CI) relies on the cooperation of the Sandia community that we support.

- CI-Help@sandia.gov
- CA & NM: 505-284-3878

Unusual Solicitation

Any attempt by any unauthorized persons to gain access to classified information is a matter of significant Counterintelligence concern and, per DOE/NNSA reporting requirements, should be reported immediately to Counterintelligence.

This applies equally to foreign nationals, as well as unauthorized U.S. citizens. Such attempts can be in the form of pointed and intrusive questions or more subtle elicitation.

This reporting requirement also applies to unusual situations that make you feel that you or a colleague is being targeted.

You must click each of the buttons to continue.

Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

BACK

Foreign Travel

Travel to sensitive countries must be reported, regardless of clearance level and/or citizenship. Clearance holders must report **all** foreign travel. As a clearance holder, foreign intelligence services may view you as a valid target by which to gain real or potential access to information of value to their governments. While in a foreign country, you remain vulnerable to foreign intelligence service tactics.

Intelligence Services may:

- Surveil your movements (audio and video coverage of your hotel room, conference room, and dining facilities)
- Enter your hotel room or other quarters at will
- Compromise your electronic devices (tap your telephone, fax machine, or laptop computer)
- Use interpreters to monitor your conversations and behaviors

You must click each of the buttons to continue.

Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

BACK

Insider Threat

Report to Counterintelligence, any individual who:

- Seeks unauthorized access to classified information, matter or special nuclear material without a Need To Know
- Appears to be living well beyond their means
- Has unreported foreign contacts or travel

Counterintelligence handles sensitive information with discretion to protect the good name and reputation of the person who is the object of your concern while balancing our responsibility to protect Sandia and national security.

Foreign intelligence services seek the cooperation of an authorized insider to betray the trust of their colleagues.

You must click each of the buttons to continue.

Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

BACK

Substantive Contact/Relationship

All Sandia MOWs, regardless of clearance and/or citizenship status, are required to report substantive contacts with foreign nationals. Substantive contact is a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds (does not include family members).

Substantive contact can be professional, personal, or financial in nature and includes ongoing contact that is solely through electronic communication (e.g., email, telephone, or social media and professional networking sites). For Sandia, substantive contact includes associations that involve meeting and the sharing of Sandia business information.

Non-U.S. citizens are considered Foreign Nationals; this includes "green card holders" or "lawful permanent residents."

You must click each of the buttons to continue.

Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

COURSE MODULES

- THE REAPPLICATION CONVERSATION ✓
- DON'T WRITE THAT DOWN ✓
- TEAMS BEHIND THE SCENES ✓
- NO CELL PHONE ZONE ✓
- A MESSAGE FROM CLASSIFICATION ✓
- COUNTERINTELLIGENCE UPDATE ✓
- **SAFEGUARDS & SECURITY UPDATE**

Safeguards & Security Update

The Safeguards and Security programs continue to seek ways to assist everyone at Sandia with their security responsibilities through policy updates, best practices, and information that can be used to protect yourself at work and at home.

The resource documents below provide additional information for the security updates in this module.

- Critical Information Lists
- Reporting Requirements & FAQs
- Controlled Articles at Sandia

You must click each of the buttons to continue.

OPSEC - Critical Information Update

Critical Information is *specific facts about Sandia's intentions, capabilities or activities vitally needed by adversaries to plan and act effectively*. Per SS013, *Critical Information Policy*, programs or centers are required to engage Sandia's OPSEC program to identify critical information specific to their work.

Unclassified government information determined by Sandia's OPSEC program to be critical information is **controlled unclassified information (CUI)** using the Operations Security category and is marked and controlled as CUI//OPSEC.

Practice OPSEC by being familiar with your critical information lists and controlling that information as CUI. All critical information lists can be accessed on the Critical Information List Library page. For more information, contact Sandia's OPSEC program at opsec@sandia.gov.

OPSEC: Critical Information Update

Reporting Requirements

Controlled Articles & CARP

BACK

Reporting Requirements Reminder

In October 2022, the DOE and Sandia Reporting Requirements of Security Interest was updated. Notable changes include a requirement for security clearance holders to report ***all* foreign travel to *any* country** for any reason, and a requirement to report ***unusual infusions of assets greater than $10,000*** (such as inheritance or winnings. Note that unusual infusions do not include every day occurrences such as sale of property, loans, stocks/tax refunds, etc).

As a Sandia-sponsored security clearance holder, it is important that you maintain an understanding of your reporting requirements, especially as they may have changed from the last time you reviewed them. For more information, see the Reporting Requirements FAQ.

For questions, or to report, contact Security Connection | 505-845-1321 or 321 from any Sandia landline phone | security@sandia.gov

You must click each of the buttons to continue.

OPSEC: Critical Information Update

Reporting Requirements

Controlled Articles & CARP

BACK

Controlled Articles & CARP

A controlled article is any electronic device capable of recording information or transmitting data, including audio, video, radio frequency, infrared, and/or data link electronic equipment. Examples include video and photography cameras, recording equipment, transmitting equipment, and more.

Per SS007, Controlled and Prohibited Articles Policy, you may not use Sandia-managed controlled articles in Limited Areas or Vault-Type Rooms (VTR) without prior authorization using the Controlled Articles Registration Process (CARP).

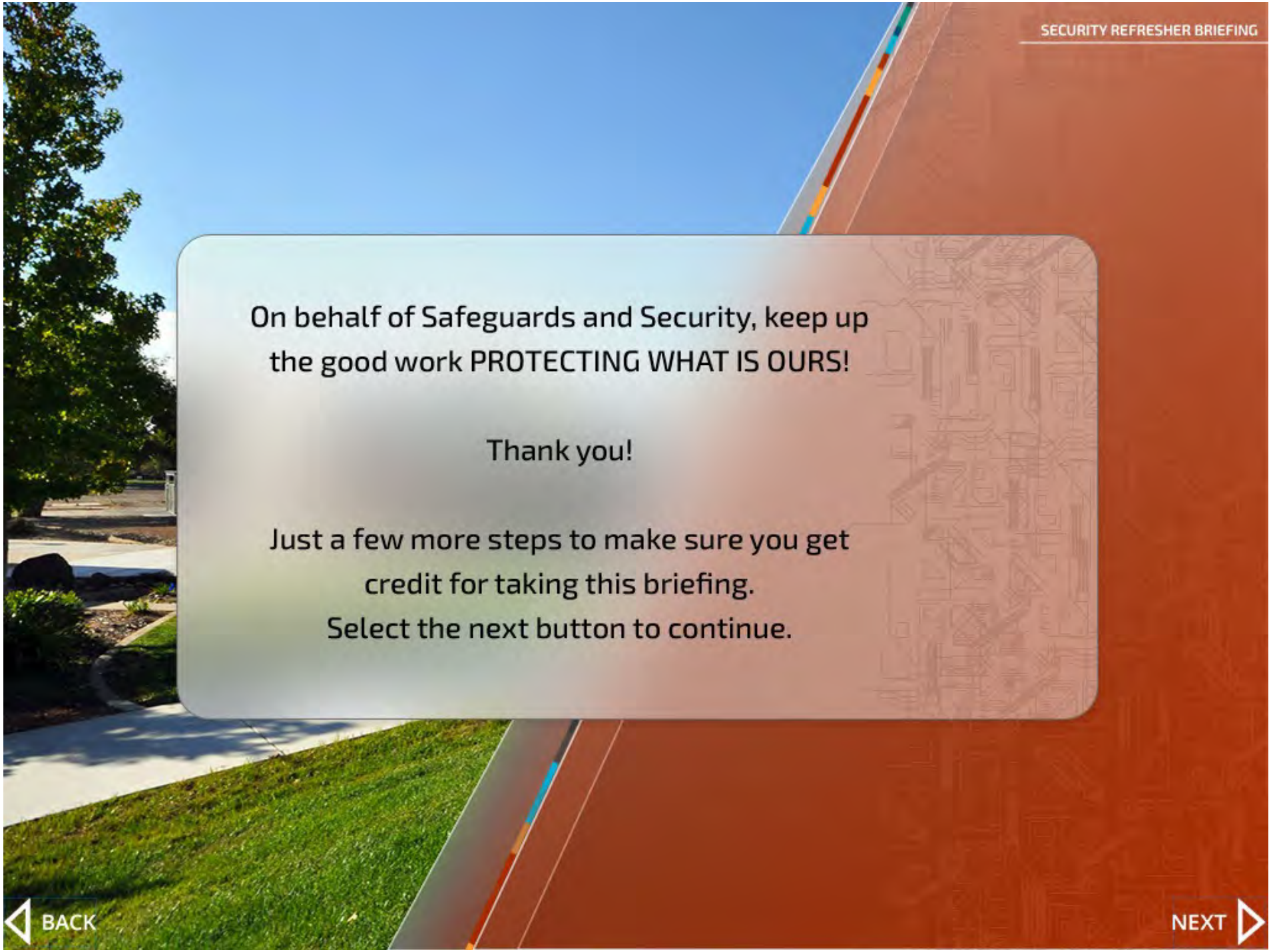
For more information, visit carp.sandia.gov or contact carp@sandia.gov.

You must click each of the buttons to continue.

OPSEC: Critical Information Update

Reporting Requirements

Controlled Articles & CARP



On behalf of Safeguards and Security, keep up the good work PROTECTING WHAT IS OURS!

Thank you!

Just a few more steps to make sure you get credit for taking this briefing.
Select the next button to continue.

SEC100 Completion Record: 2023/2024

By completing this form, you acknowledge that you have read the
Sandia National Laboratories 2023/2024 Annual Security Refresher Briefing
and understand your security responsibilities.

Complete the information below and email to securityed@sandia.gov to receive credit in the Sandia Learning Management System.

Full Name (print):	
SNL Org # or Company Name:	
Signature:	Date:
Email Address:	

For security questions or to report:
321 from a Sandia landline | 505-845-1321 from any phone
security@sandia.gov